CLAIM LISTING

The claims are listed as follows:

Claims List:

1. (Previously Presented) A system for securely transmitting data messages, comprising:

a first computer configured to transmit a data message, said data message having a header and a data portion, said first computer configured to encrypt said data portion via a first encryption technique and to encrypt said header via a second encryption technique, said first computer further configured to include information associated with said first encryption technique in said header; and

a second computer configured to receive said first data message and to decrypt said header, said second computer further configured to decrypt said data portion based on said information included in said header.

2. (Original) The system of claim 1, wherein said information associated with said first encryption technique identifies said second encryption technique.

3. (Original) The system of claim 1, wherein said second encryption technique includes RSA encryption.

4. (Original) The system of claim 3, wherein said first encryption technique includes DES encryption.

5. (Original) The system of claim 1, wherein said first computer transmits a public key to said second computer, and wherein said second computer utilizes said public key to decrypt said header.

6. (Original) The system of claim 5, wherein said first computer is configured to encrypt said public key before transmitting said public key to said second computer.

7. (Original) The system of claim 1, wherein said information associated with said first encryption technique identifies an encryption key used by said first computer to encrypt said data portion.

8. (Original) The system of claim 7, wherein said first computer randomly selects said encryption key.

9. (Original) The system of claim 1, wherein said second computer is configured to transmit a list of encryption techniques to said first computer and said first computer is configured to select said first encryption technique from said list.

10. (Original) The system of claim 9, wherein said first computer randomly selects said first encryption technique from said list.

11. (Previously Presented) A system for transmitting messages, comprising:

means for defining a data portion of a data message;

means for encrypting said data portion via a first encryption technique;

means for defining a header of said data message, said header including information associated with said first encryption technique;

means for encrypting said header via a second encryption technique;

means for transmitting said message;

means for receiving said message at a client that is remotely located from said transmitting means;

means for decrypting said header at said client; and

means for decrypting said data portion at said client based on said information in said header associated with said first encryption technique.

12. (Previously Presented) A method for transmitting messages, comprising the steps of:

defining a data portion of a first data message;

encrypting said data portion of said first data message via a first encryption technique;

defining a header of said first data message, said header of said first data message including information associated with said first encryption technique;

encrypting said header of said first data message via a second encryption technique;

transmitting said first data message subsequent to said encrypting steps

receiving said first data message at a client that is remotely located from said transmitting means;

decrypting said header at said client;

decrypting said data portion at said client based on said information in said header associated with said first encryption technique.

13. (Original) The method of claim 12, further comprising the steps of:

receiving a list of encryption techniques; and

randomly selecting said first encryption technique from said list.

14. (Original) The method of claim 12, wherein said first encryption technique includes RSA encryption.

15. (Original) The method of claim 14, wherein said second encryption technique includes DES encryption.

16. (Original) The method of claim 12, wherein said encrypting said data portion step includes the step of encrypting said data portion of said first data message with an encryption key, said method further comprising the step of including said encryption key in said header of said first data message.

17. (Original) The method of claim 16, further comprising the step of randomly selecting said encryption key.

18. (Cancelled)

19. (Original) The method of claim 16, further comprising the step of identifying said first encryption technique via information included in said header of said first data message.

20. (Original) The method of claim 16, further comprising the steps of:

transmitting a public key; and

decrypting said header of said first data message based on said public key.

21. (Original) The method of claim 20, further comprising the step of encrypting said public key before said transmitting a public key step.

22. (Original) The method of claim 12, further comprising the steps of:

defining a data portion of a second data message;

encrypting said data portion of said second data message via a third encryption technique;

defining a header of said second data message, said header of said second data message including information associated with said third encryption technique;

encrypting said header of said second data message via said second encryption technique; and

transmitting said second data message.

23. (Original) The method of claim 16, further comprising the step of randomly selecting said first and third encryption techniques.

24. (Original) The method of claim 23, further comprising the steps of:

receiving said second message;

decrypting said header of said second message; and

decrypting said data portion of said second message based on said information included in said header of said second message.

25. (Previously Presented) The system of claim 1, wherein said data message comprises a single data packet, wherein said data portion and said header are contained in said data packet.

26. (Previously Presented) The system of claim 1, wherein said information included in said header comprises decryption instructions for decrypting said data portion.

27. (Previously Presented) The system of claim 1, wherein said information included in said header comprises a key corresponding to said first encryption technique and decryption instructions for decrypting the data portion.

28. (Previously Presented) The system of claim 1, wherein said header comprises an encrypted key and said second computer is configured to decrypt said header based on said first encryption technique in order to retrieve said key, said second computer further configured to decrypt said data portion using said key.

29. (Previously Presented) The system of claim 1, wherein said information identifies a key stored at said second computer, and wherein said second computer is configured to select said key based on said information and to use said key to decrypt said data portion.

30. (Previously Presented) A method for securely communicating data messages, comprising the steps of:

receiving at a client a data packet transmitted from a server that is remotely located from said client, said data packet having a first portion encrypted via a first encryption technique and said data packet having a second portion encrypted via a second encryption technique, said second portion comprising information associated with said first encryption technique;

decrypting, at said client, said second portion to recover said information; and

decrypting, at said client, said first portion based on said information.

31. (Previously Presented) A system for securely transmitting data messages, comprising:

a first computer configured to transmit a data packet comprising a first and a second portion, said first portion encrypted by a first encryption technique and said second portion encrypted by a second technique, said second portion encrypting a public key for decrypting said first portion;

a second computer configured to receive said data packet and decrypt said second portion to generate a public key for decrypting said first portion, said second computer further configured to decrypt said first portion with said public key.

32. (Previously Presented) The system of claim 31, wherein said first computer randomly selects a first encryption technique for encrypting said data transmitted to said second computer.

33. (Previously Presented) The system of claim 32, wherein said second computer is further configured to transmit a list of encryption techniques compatible with said second computer to said first computer.

34. (Previously Presented) A method for securely transmitting data messages, comprising the steps of:

transmitting a data packet comprising a first and a second portion, said first portion encrypted by a first encryption technique and said second portion encrypted by a second technique, said second portion encrypting a public key for decrypting said first portion;

receiving said data packet by a computer;

decrypting said second portion by said computer to generate a public key for decrypting said first portion; and

decrypting said first portion by said computer with said public key.

35. (Previously Presented) The method of claim 34, further comprising the step of randomly selecting a first encryption technique for encrypting said data transmitted to said computer.

36. (Previously Presented) The method of claim 35, further comprising the step of transmitting a list of encryption techniques compatible to said computer.